2018 春 情報処理安全確保支援士 全国統一公開模試 講評と採点基準

2018 年 3 月 23 日 (株)アイテック IT 人材教育研究部

■ 全体講評

今回の公開模試における午後Ⅰ，午後Ⅱ試験の平均点は，午後Ⅰが 45.5 点，午後Ⅱが 38.2 点でした。問題別では，午後Ⅰの問 1 が 24.0 点，問 2 が 18.5 点，問 3 が 23.9 点で，問 1 の平均点が，最も高くなりました。午後Ⅱは，問 1 が 39.9 点，問 2 が 35.8 点で，問 1 の方が高い点数でした。2017 年秋期の公開模試では，午後Ⅰの平均点が 40.3 点，午後Ⅱの平均点が 42.4 点でしたから，平均点で評価すると，午後Ⅰは向上し，午後Ⅱは低下しました。また，採点結果から判断すると，本試験に向けて着実に準備が進められている受験者の方が，これまでの模試の受験者に比べると，比較的多く見られたように感じられました。

合格基準点をクリアするには，記述式の問題に対する取組み方が重要になってきます。記述式の問題の多くは，下線に関するものが出題されます。すると，解答を作成する際，どうしても下線部だけに注目しがちです。しかし，下線部だけに注目してしまうと，その前後にある条件などを見落としてしまい，的を射た答案をなかなか作成することができません。今回の模試でも，こうした答案が数多く見られました。設問で問われていることを確認した上で，下線部に関する全体の関係をよく把握し，解答を作成するようにしましょう。なお，記述式の問題においては，それぞれの設問で求める解答は基本的に一つの内容を答えさせるように条件が付けられています。このため，主語と述語，あるいは目的語は何かなどを明確にした上で解答を作成するとよいでしょう。

次に，問題ごとの選択状況を紹介しておきます。午後Ⅰ試験は，問 1（販売システムにおけるセキュリティ対策）の選択者が 46.5%，問 2（無線 LAN 環境のセキュリティ）が 22.6%，問 3（Web アプリケーションのセキュリティ対策）が 30.9%でした。このため，問 1 を選択した後，問 3 か問 2 を選択していたことになります。本試験の午後Ⅰで出題される問題数も 3 問ですから，各自が得意とする分野の問題をいち早く見つけ出し，それに集中して取り組むことが必要になると考えられます。例えば，得意分野の問題で 40 点近くの点数を獲得できれば，もう一つの問題で 20 点強を得点するだけで，午後Ⅰ試験はクリアすることができます。しかし，このようなことが可能になるには，問題の記述内容を十分に把握できるだけの知識が，まず必要とされます。本番の試験日までの期間で，より一層のレベルアップを図るとよいでしょう。

午後Ⅱ試験は，問 1（Web サービスの点検と見直し）の選択者が 58.1%，問 2（マルウェア対策）が 41.9%で，問 1 の選択者が問 2 の選択者を上回る結果となりました。午後Ⅱ試験は，様々なセキュリティ分野の知識が問われる総合問題として出題されることが多いので，できるだけ各自が得意とする分野から構成されている問題を選択するとよいでしょう。また，試験センターでは「試験結果に問題の難易差が認められた場合には，基準点の変更を行うことがあります」としています。このため，午後Ⅱ試験においては，問 1 と問 2 の難易差をあまり気にせず，一度選択すると決めた問題を最後までやり遂げることが大切です。問題選択に迷ってしまうと，2 問とも手をつけ，かえって失敗することになってしまいます。

午後Ⅰ，午後Ⅱ試験の記述式問題の多くは，問題文の中に解答を導くためのヒントが記述されています。一定の知識レベルに到達していれば，問題文で記述された内容を基にして正解を導き出すことができます。しかし，受験者によっては問題文の記述内容をそのまま引用して解答を作成している例も多く見られます。単なる引用では正解になることは極めて少ないので，設問で問われていることを十分に確認し，問題の記述内容と照らし合わせた上で論理的に考えていくようにしましょう。

試験当日は集中力，精神力，体力の勝負になります。必ず合格するという強い意志をもって，午後Ⅱ試験の最後まで全力を出し切り（あきらめずに）問題に取り組んで，ぜひ合格するようにしましょう。

＜午後Ⅰ＞

問1 販売システムにおけるセキュリティ対策

【採点基準】

[設問1]

a，b は，解答例どおりに対し各 3 点。

[設問2]

(1) c ～ f は，解答例どおりに対し各 2 点。

(2) 解答例と同様の趣旨（又は，ルート認証局をオンライン接続する必要がない旨）が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(3) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(4) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

[設問3]

(1) g，h は，解答例どおりに対し各 3 点。

(2) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（3）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

【講評】

平均点は 24.0 点（平均正答率は 48.0%）であり，午後 I の中では，最も高い点数でした。サーバ証明書の検証に関しては，おおむね理解されているようでしたが，詳細な点については，まだ不十分な面があるように見受けられました。

設問 1 は，正答率は低かったようです。空欄 a については，共通鍵ではなく，事前共有鍵などの誤答が散見されました。

設問 2 (1)の正答率は高かったようです。中間認証局とルート認証局の関係などはよく理解されていましたが，空欄 d は公開鍵ではなく，アルゴリズムという答案が散見されました。証明書の検証には公開鍵を使用しますので，基本的な事項は十分に理解しておきましょう。(2)，(3)の正答率は低かったようです。(3)については，中間攻撃者が有効期間の切れた証明書，あるいは失効した証明書を使用すれば，証明書の検証で接続が拒否されますので，攻撃自体が成り立ちません。一方，(4)の正答率は高かったです。

設問 3 (1)，(3)の正答率は高く，(2)の正答率は低かったようです。無線 LAN の暗号化と HTTPS による暗号化の関係については，よく理解されていました。

問2 無線 LAN 環境のセキュリティ

【採点基準】

［設問1］

（1）a ～ d は，解答例どおりに対し各 2 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問2］

（1）e は，解答例どおりに対し 2 点。

（2）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問3］

（1）f は，解答例どおりに対し 2 点。

（2）g，h は，解答例どおりに対し各 2 点。

（3）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

（4）解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

［設問4］

（1）解答例と同様の趣旨（キャッシュ DNS サーバとインターネットへの通信というキーワードがともに必要）が適切に指摘されているものに対し 6 点。どちらか一方の場合は 3 点。その他は 0 点。

（2）解答例と同様の趣旨（5 GHz 帯の指摘が必要）が適切に指摘されているものに対し 4 点。その他は，基本的に 0 点。

【講評】

平均点は 18.5 点（平均正答率は 37.1%）でした。平均点では，午後 I の 3 問の中で，最も低い点数にとどまりました。全体的に技術的な内容を問う設問が多かったことが，その要因と考えられます。

設問 1 (1)，(2)とも，正答率は低かったと思います。(1)の TKIP や CCMP などについては，十分に理解されていなかったようです。(2)は，無線 LAN で暗号化されたメッセージのビットを“0”から“1”，“1”から“0”に変更した際，変更したビット位置に対応する ICV のビットも変更すれば，CRC によるチェックにかからないという性質を問う問題でしたが，必ずしも十分に理解されていないようでした。

設問 2 (1)，(2)の正答率は，期待していたものよりは低かったです。(2)は，MAC アドレスや SSID などの無線通信を行う上で必要な制御情報は，暗号化されないということを覚えておくとよいかもしれません。

設問 3 (1), (2)の正答率は，やや低かったと思います。特に空欄 h に入れる鍵長の正答率は低かったと思います。暗号の安全性が保証されるのは，暗号アルゴリズムではなく，基本的に鍵長に依存していることに注意してください。(3)のポイントは，1,024 ビットの RSA を使って鍵交換を行うと，RSA の秘密鍵を推測され，TLS の暗号化で使用する共通鍵を作成される危険性があるということです。共通鍵を作成されると，それまでに行われた暗号化データが保存されていた場合には，全てのデータを解読されてしまいます。暗号化データの中に個人情報やクレジットカード番号が含まれていると大変なことになってしまいます。(4)の正答率は，まずまずでした。

設問 4 の(1)については，設問の条件が見落とされていたように感じられました。本試験では，設問などの条件を加味した上で答案を作成するように心掛けてください。

問3 Web アプリケーションのセキュリティ対策

【採点基準】

［設問1］

a，g は，解答例どおりに対し各 3 点。

［設問2］

（1）b，c は，解答例どおりに対し各 5 点。

（2）d は，解答例どおりに対し 5 点。

（3）e，fは，解答例どおりに対し各2点。
（4）hは，解答例どおりに対し5点。

［設問3］
（1）i，jは，解答例どおりに対し各2点。
（2）kは，解答例どおりに対し2点。lは，解答例と同様の趣旨が適切に指摘されているものに対し5点。その他は，基本的に0点。
（3）修正内容は，解答例と同様の趣旨が適切に指摘されているものに対し5点。その他は，基本的に0点。内容が変化するヘッダは，解答例どおりに対し4点。

【講評】

平均点は23.9点（平均正答率は47.9%）で，午後Ⅰの3問の中では，問1とほぼ同程度の高い点数でした。これまで，Web関連のセキュリティ問題は，Webサイトのセキュリティに関する知識を有している受験者に限られるといった傾向がありましたが，今回は30.9%という数字が示すように，幅広い受験者が選択する結果となりました。なお，本試験でWebサイトに関連するセキュリティ問題を選択する際には，IPAが公開している「安全なウェブサイトの作り方」などの資料を十分に学習しておく他，プログラミング言語と併せて出題されることも多いので，事前の準備を怠らないようにすることが重要です。

設問1は，まずまずの正答率でした。

設問2は，(1)を除き，かなり高い正答率でした。この結果，平均点を押し上げたものと思われます。

設問3(1)の正答率は高く，特に問題はありません。(2)の空欄lに入れる字句は，セッション固定化攻撃の手口に関するものです。他人が使用しているセッションを乗っ取るためには，攻撃者はあらかじめWebサーバから取得したセッションIDを他人に使用させることが必要です。逆に，攻撃者が任意のセッションIDを用意して，それを他人に使用させたのでは，Webサーバとのセッションが確立されていないので，他人のセッションを乗っ取ることはできません。こうした基本的な事項については，よく整理しておくとよいでしょう。(3)の正答率は，思っていたよりは低かったと思います。例えば，セッション固定化攻撃の対策については，ログイン成功後に新しいセッションIDを発行することが定石になっています。このため，容易に正解できると思っていましたが，必ずしも的確に答えられていなかったようです。

＜午後Ⅱ＞

問1　Webサービスの点検と見直し

【採点基準】

［設問1］
（1）a ～ cは，解答例どおりに対し各2点。
（2）d ～ fは，解答例どおりに対し各3点。

［設問2］
（1）解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。
（2）解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。
（3）gは，解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。

［設問3］
（1）解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。
（2）業務作業は，解答例と同様の趣旨が適切に指摘されているものに対し4点。その他は，基本的に0点。変更内容は，解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。

［設問4］
（1）解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。
（2）解答例と同様の趣旨が適切に指摘されているものに対し6点。D社用サーバLANのFWの負荷を指摘したものは3点。その他は0点。
（3）h，iは，解答例どおりに対し各3点。
（4）解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。
（5）解答例と同様の趣旨が適切に指摘されているものに対し7点。その他は，基本的に0点。

［設問5］
（1）解答例どおりに対し8点。
（2）解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。
（3）解答例と同様の趣旨が適切に指摘されているものに対し6点。その他は，基本的に0点。

【講評】

問1の平均点は39.9点で，問2の35.8点を上回る結果となりました。また，高得点の受験者もこれまでの模試に比較して多く見られたように思います。受験者も，問2に比較して取り組みやすいと感じられたのでしょう。選択者の比率でも，問1は58.1%と，問2の41.9%を上回っています。

設問1(1)，(2)の正答率は，全体的に低かったようです。(1)の攻撃の特徴などは，十分に把握しておきましょう。また，(2)のDNSキャッシュポイズニング対策においてランダム化する必要があるものは何か，DNSリフレクション攻撃への対策として有効な対策などについては，理解を深めておきましょう。

設問 2 は，まずまずの正答率だったと思います。

設問 3 (2)の Y 社の業務作業については，作業の内容ではなく，作業に関する問題点を指摘した答案が散見されました。設問で問われていることに対し，素直に答案を作成することが，点数アップにつながります。本試験では，丁寧に答案を作成するようにしましょう。

設問 4 (1)は，サーバの資源が不足する理由ではなく，TCP SYN Flood 攻撃を説明した答案が散見されました。(3)の h については，振る舞い検知などの答案も見られました。マルウェアと IPS の検知方法の違いに注意しておきましょう。(4)，(5)は，比較的正答率が良かったようですが，(4)は IPS 自体の説明や，利用する目的を答えた答案も散見されました。

設問 5 (1)は，想定以上に正答率は良かったと思います。Cookie に関する理解は，徐々に進んでいるように見受けられます。(2)は，通信制御装置の動作を問うものでしたが，動作ではなく，リバースプロキシ方式を説明した答案が散見されました。(3)も，リバースプロキシ方式によるセキュリティ上のメリットを問いましたが，SSO のメリットなどを答えた答案が散見され，正答率は低かったように思います。

問2 マルウェア対策

【採点基準】

[設問1]

(1) a ～ d は，解答例どおりに対し各 2 点。

(2) e ～ g は，解答例どおりに対し各 3 点。

(3) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は，基本的に 0 点。

(4) 解答例と同様の趣旨が適切に指摘されているものに対し 8 点。その他は，基本的に 0 点。

[設問2]

(1) 解答例と同様の趣旨が適切に指摘されているものに対し各 5 点。その他は，基本的に 0 点。

(2) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(3) h ～ j は，解答例どおりに対し各 2 点。

(4) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。「L3SW とファイルサーバは固定 IP アドレス」，「PC は相互に通信しない」のうち，いずれか一方を指摘したものは 3 点。その他は 0 点。

(5) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(6) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

[設問3]

(1) 解答例どおりに対し 3 点。

(2) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(3) 解答例と同様の趣旨が適切に指摘されているものに対し 6 点。その他は，基本的に 0 点。

(4) 脅威，対策とも，解答例と同様の趣旨が適切に指摘されているものに対し各 6 点。その他は，基本的に 0 点。

【講評】

問 2 の平均点は 35.8 点であり，問 1 より 4.1 点低くなりました。設問に答えるための条件が，問題全体に散りばめられていたことなどから，条件を考慮した解答が的確に作成できなかったものと思われます。また，少し技術的な出題内容になっていたことなどから，選択者数も問 1 の 58.1%より少なく，41.9%でした。

設問 1 (1)は，正答率が低かったようです。メールサーバの設定については，送信者と受信者の関係などを明確にして考えましょう。(2)の送信ドメイン認証についても，まだ十分に理解されていないようです。認証する仕組み自体に関する知識は重要ですから，理解を深めましょう。(3)，(4)は，送信ドメイン認証の新しい仕組みである DMARC に関する問題を出題しましたが，既に一部の受験者はよく理解されていました。

設問 2 (1)，(2)は，想定していたよりも正答率が低かったと思います。プロキシサーバで利用者認証が行われている場合には，マルウェアは利用者認証に成功しないと，プロキシサーバを利用できません。また，URL フィルタリングはプロキシサーバがもつ機能ですから，こうした知識を一つ一つ積み上げていくことも必要です。(3)は，ARP ポイズニングの基本的な問題ですから，丁寧に取り組むようにしましょう。(5)の正答率は，比較的高かった半面，(6)は情報を流出されると脅すランサムウェアという条件が考慮されず，単にデータのバックアップと解答した答案が多く見られました。

設問 3 (1)は，SSH のパスワード認証よりも安全な認証方式を問いましたが，公開鍵認証という答案は限られていました。(2)は，SSH のポート番号を変更する旨の解答を求めましたが，サーバで稼働していないポートを閉じるなどの答案が散見されました。また，ポートという字句は，サーバのサービスポートを意味する場合と，設問 2 (5)のように L2SW の接続ポートを意味する場合があります。(4)は，マルウェア感染に着目した答案が見られましたが，問題ではマルウェア以外の留意事項について検討するという文脈になっています。このため，最近話題になっている IoT 家電への不正アクセスや不正操作などに着目してほしかったと思います。

以上